Onderzoek Office 365

Gemeente Breda

14 juni 2016

Referentie: 20160614\_Onderzoek\_Office365\_v1.docx

**Onderzoek Office 365 bij gemeente Breda**

**Context**  
De gemeente Breda onderzoekt de mogelijkheden om Office 365 breed te gaan gebruiken in de organisatie. Hierin spelen naast functionele aspecten ook beveiliging- en privacyaspecten een belangrijke rol. Aangezien de leverancier Microsoft een Amerikaanse partij is met datacenter locaties over de gehele wereld, rijst met name de vraag of de Europese en/of Nederlandse privacywetgeving het – met het oog op anti-privacy wetgeving als de Patriot act – toestaat om met persoonsgegevens van Nederlanders te werken in de Cloud omgeving van Microsoft.

Naast de vraag over de risico’s op het gebied van privacy, zijn in de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) ook een aantal normen voor beveiliging opgenomen, waaraan de Vereniging van Nederlandse Gemeenten zich heeft gecommitteerd.   
  
Ook gemeente Breda heeft zich gecommitteerd om aan de BIG te voldoen. Conform de BIG kunnen uitzonderingen op maatregelen worden toegestaan op basis van een risico afweging en akkoord op het aanvaarden van het risico door het betreffende management. Dit wordt vastgelegd in een risico statement. Ook wanneer dermate grote risico’s worden geïdentificeerd dat ze een grote kans van manifesteren hebben en deze bij manifestatie een grote impact hebben, worden deze opgenomen in het risico statement.

**Onderzoekstappen**  
Het onderzoek heeft plaatsgevonden op de volgende vlakken van de Office 365 oplossing:

1. *Wet- en regelgeving*

Wanneer data van bedrijven in de Cloud geplaatst worden, dient een aantal aspecten in overweging genomen te worden. Dit betreft de geldende privacywetgeving (zowel de Europese Privacy Verordening, als de Wet bescherming persoonsgegevens (Wbp)). Tevens dient hier de in 2018 van kracht wordende Europese Privacy Verordening in ogenschouw genomen te worden. Dit alles is met name van belang in het kader van specifieke buitenlandse wetgeving, zoals Patriot act, die overheden mogelijkheden geven om in bepaalde gevallen data van bedrijven te vorderen en in te zien. Genoemde wet- en regelgeving is uitvoerig onderzocht en beschouwd in het kader van dit onderzoek. Ook is de bestaande overeenkomst met leverancier SoftwareOne beoordeeld op dit onderwerp.

1. *Informatiebeveiliging, security en maatregelen*

Om een duidelijk inzicht te krijgen in de staat van de security en (informatie)beveiligingsmaatregelen, die van toepassing zijn op de Microsoft Cloud-omgeving, is onderzoek gedaan naar de maatregelen, die Microsoft heeft toegepast en welke maatregelen Microsoft niet heeft toegepast. Er is telefonisch contact geweest met Sander de Graaf van Centric. Centric heeft veel klanten binnen de overheidssector. Omdat overheden een sceptische houding hebben ten op zichtte van het gebruik van Public Clouddiensten, is Centric terughoudend in het gebruik hiervan binnen hun productlijnen. Tevens is de GAP met de BIG in kaart gebracht en is een inschatting gemaakt welke van de resterende maatregelen al door de gemeente Breda zelf zijn ingericht (en voldoende dekkend zijn).

1. *Functionaliteit en proces*

De inrichting van Cloud services, zoals Office 365, kan beperkingen opleggen aan functionaliteiten van applicaties. Integratie van de nieuwste versie van het Office-pakket kan incompatibel zijn met bestaande software en daarmee beperkingen opleggen aan de functionaliteit van de software, wanneer deze afhankelijk is van bepaalde office toepassingen. In het kader van dit onderzoek zijn mogelijke incompatibiliteitsissues nader bestudeerd en waar van toepassing geïdentificeerd.

**Bevindingen**

Gedurende het onderzoek zijn de volgende zaken aan het licht gekomen:

1. Wet -en regelgeving

Microsoft werkt conform de richtlijnen van de EU privacy werkgroep Artikel 29 met EU model clausules. Microsoft hanteert het beleid dat data van klanten versleuteld wordt en niet wordt doorgegeven aan anderen dan de eigenaar. Dit houdt ook in dat wanneer de Amerikaanse overheid data vordert, Microsoft deze niet afgeeft en de Amerikaanse overheid doorverwijst naar de organisatie, waarvan ze de data wil ontvangen. Wanneer genoemde clausules zijn opgenomen in de overeenkomst en verdere afspraken met Microsoft zijn gemaakt conform voor beide partijen acceptabele voorwaarden, dan zijn er geen beperkingen in het kader van de Wbp. Nader onderzoek naar de bestaande overeenkomst met Microsoft (SoftwareOne) wijst uit dat de model clausules niet zijn opgenomen. Voor zover wij hebben kunnen beoordelen beperkt deze overeenkomst zich tot een licentieovereenkomst.

1. Informatiebeveiliging, security en maatregelen

De Microsoft Cloud is op diverse manieren beveiligd. Iedere klantomgeving is gescheiden van andere klantomgevingen, zodat anderen niet bij de data van de klant kunnen komen. Tevens is verkeer over verbindingen versleuteld en wordt gescand op virussen en malware. Authenticatie vindt plaats via AD Federation Services, wat betekent dat medewerkers kunnen inloggen met hun reguliere Microsoft Active Directory account. De autorisaties op bestanden en toegang tot accounts kan ingericht worden, conform de regels en richtlijnen van de klant (gemeente Breda).

1. Functionaliteit en proces

Bekende incompatibiliteitsissues hebben betrekking op de integratie van Microsoft Office toepassingen met applicaties. Wanneer de Office toepassing wordt aangeroepen door de applicatie, wordt de Office toepassing opgestart. Dit gebeurt door een hard geprogrammeerde regel code, die niet verandert, wanneer het aanroep commando van de Office toepassing (bijvoorbeeld door een update door Microsoft) wel verandert. Hierdoor werkt het aanroepen van de Office toepassing vervolgens niet meer correct met gevolgen voor het functioneren van de applicatie. Binnen het applicatielandschap van gemeente Breda zijn zulke toepassingen bekend met ITP van PinkRoccade (BZ en Belastingen) en Doc4All / Key2Documentenuitvoer van Centric (zaaksysteem/DMS, GWS en PNA). Om de specifieke impact per applicatie en bijbehorende maatregelen te bepalen, dient nader onderzoek plaats te vinden naar de integratie met (minimaal) genoemde applicaties en andere applicaties, waarop dit van toepassing is. De huidige opzet van het implementatieplan van Office 365 voorziet erin dat de applicatieservers blijven functioneren met de huidige Office-versie. Deze worden niet gemigreerd naar Office 365. De Office-versies op de werkplek worden wel gemigreerd naar Office 365. Hiervoor zijn de risico’s echter zeer beperkt / verwaarloosbaar.

**Aanbevelingen**

1. Het verdient aanbeveling dat de gemeente Breda voordat het Microsoft Office 365 breed gaat gebruiken binnen de organisatie, minimaal de volgende onderdelen op laat nemen in de overeenkomst met Microsoft: Service Level Agreement, EU model clausules en, indien noodzakelijk, aanvullend een bewerkersovereenkomst. De onderdelen van de BIG dienen hierin afgedekt te zijn. Zoals aangegeven dienen deze onderdelen opgenomen te zijn, om aan wet- en regelgeving te voldoen. Zonder deze model clausules voldoet Office 365 niet aan de Wbp en mogen geen persoonsgegevens worden bewerkt met Office 365.   
     
   *De volgende documenten zijn in een later stadium alsnog aangeleverd:*
   1. *Enrollment Agreement – Enterprise.docx*
   2. *Enrollment Agreement.docx*
   3. *Master Agreement.docx*
   4. *MicrosoftOnlineServicesTerms(Dutch)(May2016)*
   5. *Signature Form.docx*
   6. *Bevestiging van de acceptatie en indiening van Microsoft-volumelicentieovereenkomst(en){~749324181~}*

*Bovenstaande documenten zijn digitaal gegenereerd en ondertekend. Het document “Signature Form.docx” is het formulier voor de overeenkomst. Deze is niet ondertekend. Bijgevoegde email bevestiging met de naam “Bevestiging van de acceptatie en indiening van Microsoft-Volumelicentieovereenkomst(en) 749324181” aan het voormalig hoofd Servicebedrijf maken de overeenkomst rechtsgeldig. In het document “Enrollment Agreement – Enterprise.docx” worden de volgende in de aanbeveling genoemde onderdelen opgenomen:*

* *EU model clausules met betrekking tot privacy bewerkersovereenkomst   
  (dit heet verwerkersovereenkomst in dit document).*
* *De overeenkomst voorziet in een Microsoft standaard Service Level Agreement voor Online Diensten, Azure en niet voor: MS Social Engagement, MS Dynamics, Marketing, MS Parature, MS Advanced Theat Protection, MS Project Pro, MS Visio Pro, Delve Analytics, Advanced eDiscovery.*

*Indien deze diensten niet worden gebruikt vormt dit geen risico.*

***Hiermee voldoet de overeenkomst samen met alle hierboven genoemde documenten aan de in de aanbeveling onder 1 genoemde voorwaarden****.*

1. Ook bevelen wij de gemeente aan om de aanbevelingen uit de eerder uitgevoerde GAP-analyse uit te voeren om bestaande interne beveiligingsmaatregelen voor de Office 365 applicaties en waar nodig (bestaande of nieuwe) procedures aan te passen op het veilig gebruik van de Cloud omgeving. Het uitgevoerde onderzoek wijst uit dat de technische maatregelen die door Microsoft zijn ingericht, de technische maatregelen in de BIG grotendeels afdekken. Belangrijke aandachtspunten, die opgepakt dienen te worden bij gebruik van Office 365 zijn encryptie van de data op de harde schijf op de werkplek, waar data lokaal kan worden opgeslagen, inrichting van AD Federation Services (of vergelijkbaar) voor eenduidige gebruikerstoegang, two-factor authenticatie voor benadering door thuisgebruikers en invoering van data classificatie om de ongeautoriseerde en ongewenste verspreiding van gevoelige informatie op het Internet (via Sharepoint Online of MS Drive) tegen te gaan. Daarnaast is awareness bij de gebruiker noodzakelijk om op de juiste manier met gevoelige data om te gaan. Awareness bij de medewerkers van gemeente Breda is laag. Wij bevelen aan een degelijke awareness campagne op te zetten en uit te voeren voor de gehele organisatie.   
     
   *Actiepunten:*
   1. *Onderzoek naar de mogelijkheden om informatie opgeslagen op (mobiele) gegevensdragers[[1]](#footnote-1) ontoegankelijk kan worden gemaakt voor onbevoegden in het geval van diefstal of verlies (encryptie).*
   2. *Documentatie en (technische) inrichting (architectuur) van Active Directory Federation Services (ADFS); het betreft een volledige subset van de identificatie en authenticatie gegevens van gemeente Breda, welke met passende maatregelen moet worden beschermd.*
   3. *Documentatie en (technische) inrichting (architectuur) van Office 365 Policy’s en instellingen; het is bijvoorbeeld mogelijk om het delen van documenten via SharePoint Online te beperken tot de eigen organisatie. Het documenteren en beargumenteren van keuzes in deze policy’s is essentieel om te beoordelen welke maatregelen zijn getroffen.*
   4. *Onderzoek naar het gebruik van Two-Factor authenticatie voor onderdelen van de Office 365 omgeving, met name voor gebruik buiten de organisatie; intern is dit minder relevant en zelfs in het geval van PIP niet wenselijk. Bij gebruik buiten de organisatie verdient het gebruik van Two Factor authenticatie sterk de aanbeveling.*
   5. *Om de bewustwording onder gebruikers te vergroten zal er komend jaar een awareness campagne plaats vinden, waarbij minimaal een presentatie met betrekking tot privacy en informatiebeveiliging in het werkoverleg van diverse directies zal worden gegeven. Tevens is het de bedoeling een Strategische leerlijn Informatievaardigheden via HR.(YourGoals) op te zetten. Het gebruik van Clouddiensten krijgt daar ook de aandacht. Men zal het document “VerklaringInformatieGebruik” moeten ondertekenen (moet nog worden vastgesteld!),waarin wordt aangegeven hoe binnen gemeente Breda met informatie moet worden omgegaan. Tevens krijgt men bij deze verklaring een A4 met Infographic mee met de risico’s met betrekking tot het werken in de cloud / buiten de organisatie.*
2. Momenteel is niet voorzien in het migreren van lokale Office-versies, die met applicaties geïntegreerd zijn. Deze lokale Office-versies op (applicatie)servers blijven in de huidige vorm gehandhaafd. Mocht dit in de toekomst wel gewenste of noodzakelijk zijn, dan zouden wij aanbevelen – om het juist functioneren van applicaties in de Cloud te kunnen garanderen – om een breder onderzoek in te stellen naar de specifieke applicaties die in de Office 365 omgeving gebruikt gaan worden. Op deze manier kan per applicatie een overzicht van aandachtspunten verkregen worden, waarmee de applicatie in de Cloud omgeving optimaal kan functioneren. Zoals aangegeven, zijn er op dit moment geen applicaties bekend, waarbij sprake is van (verregaande) integratie van Office.

*Er is gekozen om office integratie binnen applicaties voorlopig niet op te pakken, maar dit op de huidige versie te handhaven en eventueel mee te scripten met de betreffende applicatie in de ‘virtuele software bubble’ (softgrid).*

**Afweging**

Met het implementeren van de hiervoor benoemde aanbevelingen voldoet de gemeente Breda aan alle geldende wet- en regelgeving op het gebied van privacy en informatiebeveiliging, zoals vastgesteld en van toepassing op genoemde aspecten.

Echter, ondanks alle rechten en afspraken, die gemaakt zijn in dit kader, kan het voorkomen dat overheidsdiensten van landen buiten de EU vordering eisen en/of forceren van de gegevens van de gemeente Breda. Dit risico valt in de huidige setup van de Clouddienst van Microsoft niet geheel uit te sluiten. Wij achten echter op dit moment het reële risico dat hiermee gemoeid is zeer beperkt. Ook navraag bij zowel Microsoft, als andere bedrijven en (overheid)instellingen, bevestigen dit. Daarbij geeft Microsoft aan geen data over te dragen van klanten, maar verwijst zij de aanvragende instantie (in het kader van de Patriot act zou dit de overheid van de Verenigde Staten zijn) naar de eigenaar van de data.

**Afwijking van de norm**

Er is geen afwijking van de norm geconstateerd, indien en slechts dan als eerdergenoemde aanbevelingen worden opgevolgd.

**Voorwaarden**

Indien:

1. Een onafhankelijk auditor zou vaststellen, dat de afwijking van de norm dermate grote risico’s met zich meebrengt, waardoor gemeente Breda niet zou slagen voor een audit en daarmee een benodigde verklaring niet kan worden afgegeven, of;
2. Wordt geconstateerd of vernomen dat genoemde aanbevelingen niet zijn toegepast en / of geldende wet- en regelgeving niet consequent wordt gevolgd.

kan dit verstrekkende gevolgen hebben voor het imago van gemeente Breda en kunnen grote boetes het gevolg zijn. Het management van PI, als opdrachtgever namens Servicebedrijf, is hiervan op de hoogte gebracht en is hiermee bekend en accepteert de beschreven risico’s.

1. *Onder (mobiele) gegevensdragers worden laptops, pc’s, usb-sticks, tablets en externe harddisks verstaan.* [↑](#footnote-ref-1)